Executable-Icon-Location

Carefully manage destination buffer size

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 5382 bytes

<table>
<tr><td><b>Attack Category</b></td><td><ul><li>Malicious Input</li><li>Path spoofing or confusion problem</li></ul></td></tr>
<tr><td><b>Vulnerability Category</b></td><td><ul><li>Buffer Overflow</li><li>Input source (not really attack)</li><li>Unconditional</li></ul></td></tr>
<tr><td><b>Software Context</b></td><td><ul><li>Shell Functions</li><li>File Management</li></ul></td></tr>
<tr><td><b>Location</b></td><td><ul><li>shellapi.h</li></ul></td></tr>
<tr><td><b>Description</b></td><td>When calling functions for locating files and icons, the destination string buffer must be long enough to hold the return file path. Otherwise, buffer overflows will occur.</td></tr>
<tr><td><b>APIs</b></td><td>
<table>
<tr><th>Function Name</th><th>Comments</th></tr>
<tr><td>ExtractAssociatedIcon</td><td>lpIconPath [in/out], read from file</td></tr>
<tr><td>ExtractAssociatedIconA</td><td>lpIconPath [in/out], read from file</td></tr>
<tr><td>ExtractAssociatedIconEx</td><td>Second param: lpIconPath</td></tr>
<tr><td>ExtractAssociatedIconExA</td><td>Second param: lpIconPath</td></tr>
<tr><td>ExtractAssociatedIconExW</td><td>Second param: lpIconPath</td></tr>
<tr><td>ExtractAssociatedIconW</td><td>lpIconPath [in/out], read from file</td></tr>
<tr><td>FindExecutable</td><td>Last parameter: lpResult</td></tr>
<tr><td>FindExecutableA</td><td>Last parameter: lpResult</td></tr>
<tr><td>FindExecutableW</td><td>Last parameter: lpResult</td></tr>
<tr><td>AssocQueryString</td><td>Second to last parameter: pszOut</td></tr>
</table>
</td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

<table>
<tr><td><b>Method of Attack</b></td><td>These routines are all subject to buffer overflows. If the attacker provides a long path name, it could overflow a buffer that is not at least MAX_PATH characters in length.</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td>
<table>
<tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr>
<tr><td>When any of the indicated functions is called.</td><td>The specified parameter must be at least MAX_PATH characters in length to ensure that it is large enough to hold the returned string. Otherwise, a buffer overflow can occur.
[Actually, the documentation does not specify the maximum size for lpIconPath, but we assume MAX_PATH as it is the maximum length of an ASCII file path in Windows. Note that when Unicode is in use, some functions allow paths far larger than MAX_PATH, provided they begin with the special sequence "\\?\". Check documentation to determine whether your code needs to allow for this possibility.]</td><td>Effective, subject to issue of Unicode paths that may exceed MAX_PATH characters in length.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td><b>Signature Details</b></td><td>Any of the indicated functions is called.</td></tr>
<tr><td><b>Examples of Incorrect Code</b></td><td><code>TCHAR lpResult[20]; // Buffer is too small</code>
<code>// Note: FindExecutable is, strangely, for finding files but not for finding executables</code>
<code>HINSTANCE instance =</code>
<code>FindExecutable(</code>
<code>TEXT("MyFile.txt"),</code>
<code>TEXT("C:\\MyDirectory"),</code>
<code>LPTSTR lpResult</code>
<code>);</code></td></tr>
<tr><td><b>Examples of Corrected Code</b></td><td><code>TCHAR lpResult[MAX_PATH]; // Buffer is correctly sized</code>
<code>// Note: FindExecutable is, strangely, for finding files but not for finding executables</code>
<code>HINSTANCE instance =</code>
<code>FindExecutable(</code>
<code>TEXT("MyFile.txt"),</code>
<code>TEXT("C:\\MyDirectory"),</code>
<code>LPTSTR lpResult</code>
<code>);</code></td></tr>
<tr><td><b>Source Reference</b></td><td>http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/findexecutable.asp[2]</td></tr>
<tr><td><b>Recommended Resource</b></td><td></td></tr>
<tr><td><b>Discriminant Set</b></td><td><table><tr><td><b>Operating System</b></td><td>• Windows</td></tr><tr><td><b>Languages</b></td><td>• C
• C++</td></tr></table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com